Cascadia Intellectual Property
500 Union Street
Suite 1005
Seattle, Washington 98101
Telephone: (206) 381-3900
Facsimile: (206) 381-3999

Facsimile Transmittal

To: Board of Patent Appeals and Interferences **Fax:** (571) 273-8300

From: Patrick J.S. Inouye **Date:** November 14, 2006

Re: Appeal Brief
Serial No. 09/346,559 **Pages:** 22 (including cover sheet)

CC:

☐ **Urgent** ☐ **For Review** ☐ **Please Comment** ☐ **Please Reply** ☐ **Please Recycle**

Notes: Regarding the above-identified U.S. Patent Application, please find attached hereto:

- Transmittal Form
- Appeal Brief

RECEIVED
CENTRAL FAX CENTER

NOV 14 2006

PTO/SB/21 (09-06)
Approved for use through 4/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paper Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

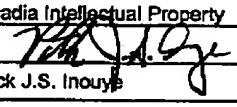
TRANSMITTAL FORM (to be used for all correspondence after initial filing)			
		Application Number	09/346,559
		Filing Date	December 11, 2002
		First Named Inventor	Goldberg, David
		Art Unit	2625
		Examiner Name	James A. Thompson
Total Number of Pages in This Submission		Attorney Docket Number	D/99176

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
- ☐ Fee Attached
- ☐ Amendment / Reply
- ☐ After Final
- ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
- ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ Landscape Table on CD
- ☐ After Allowance communication to (TC)
- ☒ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Cascadia Intellectual Property		
Signature			
Printed name	Patrick J.S. Inouye		
Date	November 14, 2006	Reg. No.	40,297

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature			
Typed or printed name	Krista Wittman	Date	November 14, 2006

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED
CENTRAL FAX CENTER
NOV 14 2006

Appeal Brief
Docket No. D/99176

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Goldberg, et al.	Group Art Unit: 2625
Serial No. 09/346,559	Examiner: James A. Thompson
Filed: December 11, 2002	
For: System For Authenticating Hardcopy Documents	

APPEAL BRIEF

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON BEHALF OF GOLDBERG, ET AL.:

Appellant appeals from the Office Action mailed, June 5, 2006, in which currently-pending claims 1-23 stand rejected. Appellant filed a Notice of Appeal with a one-month extension of time by facsimile on September 14, 2006 to reinstate the earlier appeal of December 5, 2003.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is assignee Xerox Corporation, a New York Corporation, located at 800 Long Ridge Road, P.O. Box 1600, Stamford, CT 06904-1600.

2. RELATED APPEALS AND INTERFERENCES

A first Notice of Appeal was filed on December 5, 2003. A timely Appeal Brief was filed on February 5, 2004. Following a return to *ex parte* prosecution, a Supplemental Appeal Brief was filed on July 22, 2004 to reinstate the appeal. A Notice of Appeal was not filed to reinstate the appeal of July 22, 2004, but the Supplemental Appeal Brief was entered by the leave of the Examiner. Following a second return to *ex parte* prosecution, a second Notice of Appeal was filed on September 14, 2006 to reinstate the appeal and this Appeal Brief is being submitted as part of that reinstatement request. There are no other appeals or interferences known to Appellant, Appellant's legal counsel, or assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

Claims 1-23 are pending. Claims 1-23 stand rejected and are the subject of this appeal. An Appendix setting forth the Claims involved in the appeal is included as Section 8 of this Appeal Brief.

4. STATUS OF AMENDMENTS

No amendments were filed subsequent to the rejection of Claims 1-23. Claims 1-23 remain pending.

5. SUMMARY OF CLAIMED SUBJECT MATTER

A. Background

The invention is addressing the problem of authenticating hardcopy documents in printed form. The problems faced in the authentication of hardcopy documents is succinctly explained in the Background and primarily relate to the non-reproducibility of scanned images, that is, two scanned bitmap images of the same hardcopy document will, at a digital level, invariably differ in terms of absolute bitwise values. Digital images, however, do not differ when reproduced.

The irreproducibility of scanned-in hardcopy documents makes for a much more difficult authentication problem, which is addressed in the invention by introducing a halftone encoding of an authentication token that contains a digital signature. A sender can physically scan in a hardcopy document, generate a digital signature based on the scanned-in representation of the document using his or her private key, and embed a digital encoding of the digital signature, using, for instance, halftone glyphs, to create a "signed and authenticated hardcopy document" that is created when the scanned-in document with embedded digital signature is "rendered," that is, printed. As a result, the digital signature, through the embedded digital encoding, becomes a part of the physically printed hardcopy document and can be used to authenticate the hardcopy document when the hardcopy document is again scanned in.

B. Independent Claim 1

Claim 1 defines a method for authenticating a hardcopy document including recording in a memory a scanned representation of the hardcopy document at a selected resolution. Lossy compressed image data is generated from the scanned representation to create an authentication token (p. 6, lines 24-28; p. 7, lines 20-29). The authentication token includes one of encrypted image data and hashed encrypted image data (p. 8, lines 1-3). The hashed encrypted image data includes the lossy compressed image data and an encrypted hash of the lossy compressed image data (p. 8, lines 3-16; p. 11, lines 25-28). The scanned representation of the hardcopy document with a digital encoding of the

authentication token is arranged for rendering at a printer a signed hardcopy document (p. 8, lines 17-19; p. 11, lines 4-15).

C. Independent Claim 18

Claim 18 defines a method for authenticating a hardcopy document including recording in a memory a scanned representation of the hardcopy document at a selected resolution. Lossy compressed image data is generated from the scanned representation to create an authentication token (p. 6, lines 24-28; p. 7, lines 20-29). The authentication token includes one of encrypted image data and hashed encrypted image data (p. 8, lines 1-3). The hashed encrypted image data includes the lossy compressed image data and an encrypted hash of the lossy compressed image data (p. 8, lines 3-16; p. 11, lines 25-28). The scanned representation of the hardcopy with a digital encoding of the authentication token is arranged for rendering at a printer a label containing the digital encoding of the authentication token (p. 15, line 24-p. 16, line 2).

D. Independent Claim 21

Independent Claim 21 defines a system for authenticating a scanned representation of a hardcopy document including an image compression module, an authentication token generator, and an encoding module. The image compression module generates lossy compressed image data from a scanned representation of a hardcopy document (p. 6, lines 24-28; p. 17, lines 20-29). The authentication token generator produces an authentication token with the lossy compressed image data including one of encrypted image data and hashed encrypted image data (p. 8, lines 1-3). The hashed encrypted image data includes the lossy compressed image data and an encrypted hash of the lossy compressed image data (p. 8, lines 3-16; p. 11, lines 25-28). The encoding module arranges the scanned representation of the hardcopy document with a digital encoding of the authentication data for rendering at a printer a signed hardcopy document (p. 8, lines 17-19; p. 11, lines 4-15).

6. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

A. Issue I

Whether Claims 1-3, 5, 7-8, 12-13, and 21-23 stand properly rejected under 35 U.S.C. § 102(e) as anticipated by Squilla.

B. Issue II

Whether Claim 4 stands properly rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla in view of Merkle.

C. Issue III

Whether Claims 6 and 9-11 stand properly rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla in view of Curry.

D. Issue IV

Whether Claims 14-17 stand properly rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla in view of Zdybel.

E. Issue V

Whether Claims 18-20 stand properly rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla in view of Walker.

7. ARGUMENT

A. U.S. Patent No. 5,898,779 ("Squilla")

Squilla discloses an encryption system for authenticating electronically-stored images using a digital camera with a private key. In the signing process, a digital image is captured and a region of interest is selected from the image for compressing and hashing (Col. 8, lines 35-40). Next, information from the photographer is appended to the hashed data and together, the hashed data and the photographer's information is encrypted to form a digital signature using a private key embedded in the digital camera. The original image remains unaltered during generation of the digital signature (Col. 7, lines 21-24). A digital signature is appended to the digital file of the original image (Col. 7, lines 55-58). The output

data of the digital file includes a header field with the location of the selected pixels for digital authentication, a signature field for the digital signature, and a data field for the digital image (Col. 5, lines 41-50).

During the authentication process, the digital signature is separated from the digital image and unencrypted header information (Col. 7, lines 59-66). The header information is used to find the location of the region of interest on the digital image previously selected for a new hashing (Col. 8, lines 4-10). The digital signature is decrypted with a public key corresponding to the private key embedded in the digital camera, which reproduces the original hashed region of interest (Col. 8, lines 11-13). The new hash and the original hash are compared to determine whether the image has been altered. If the new hash value is identical to the decrypted hash value, the image is authentic; however, if the hashes do not match, the image content is invalid (Col. 8, lines 13-19; Fig. 6).

B. U.S. Patent No. 5,157,726 ("Merkle")

Merkle discloses a system for authenticating a hardcopy of an original document using a signing copy machine and an identification card. A person copying a document activates the copy machine by placing their identification card into the signing copier (Col. 4, lines 50-59), which digitizes the document and generates a digital signature from the digitized document using a private key (Col. 4, lines 26-42). The digital signature is affixed to the hardcopy produced by the signing copier machine (Col. 4, lines 63-66) and includes information from the identification card and the hardcopy document (Col. 4, lines 42-46). The digitally-signed hardcopy is sent to a third party and placed into a second signing copier, which digitizes the hardcopy document with the digital signature and validates the digital signature via a checking algorithm (Col. 5, lines 11-14). The output of the second signing copier is a digitally cleaned document (Col. 5, lines 36-41).

C. U.S. Patent No. 5,946,103 ("Curry")

Curry discloses a method for verifying the originality of printed documents. Predetermined information is embedded in original hardcopy

documents in at least one halftone pattern that is composed of halftone cells (Col. 2, lines 49-52). Each cell includes a fill pattern that is symmetric about a central axis of the cell (Col. 5, lines 18-21). The predetermined information is represented by the angular orientations of the axis of symmetry of each cell (Col. 5, lines 21-26). The documents are classified as "originals" if the predetermined information can be successfully recovered from the embedded information (Col. 2, lines 52-55).

D. U.S. Patent No. 5,486,686 ("Zdybel")

Zdybel discloses an electronic document processing system for capturing and communicating digital data, including the structure and content of an electronic source document. A scanner inputs hardcopy documents and converts the document into an electronic bitmap (Col. 7, lines 62-65). Recognition software further converts the bitmap into elemental textual and graphical encodings (Col. 7, line 66-Col. 8, line 1). The bit level data of the textual encodings are then converted into glyph encodings (Col. 8, lines 38-47). Glyph encodings are used to recover data that affects the appearance of the document and data that is not inferable from the appearance of the document alone (Col. 9, lines 46-53). Information converted into glyph encoded data may include machine readable descriptions of data points for structured graphics, algorithms for performing computations, hypertext pointer values, structural characteristics of the electronic source document, a document editor used to prepare the source document, the file name and storage location of the electronic source document, and audit-trail data for the electronic source document (Col. 10, lines 13-27). The glyph encodings are merged into an electronic document description file for printing on a hardcopy output document (Col. 8, lines 47-50).

E. U.S. Patent No. 6,111,953 ("Walker")

Walker discloses a system for authenticating and verifying documents by affixing a representation of encrypted data on the document. Variable document data is selected and entered by a user and stored in a computer with a private key (Col. 5, lines 4-8). A cryptoprocessor encrypts the document data with the private

key to generate a unique encrypted, authentication code in a human-readable string of characters for the document (Col. 5, lines 9-11; Col. 6, lines 9-11). The central processing unit (CPU) then transmits the code to a stamper, which affixes the code onto the hardcopy document (Col. 5, lines 12-13).

During verification, the variable document data, the public key, and the encrypted code are input (Col. 6, lines 16-27). A cryptoprocessor uses the public key to decipher the encrypted code, yielding the document authentication data, which is compared to the variable document data (Col. 6, lines 23-31). The document is authentic if the document authentication data agrees with the variable document data. The system may display the authentication determination by flashing "YES" or "NO," or the CPU may output the data to a display for the user (Col. 6, lines 37-42).

F. Issue I

A *prima facie* case of anticipation under 35 U.S.C. § 102(e) has not been shown and the rejection of Claims 1-3, 5, 7-8, 12-13, and 21-23 cannot stand.

1. Legal Basis

A claim is anticipated under 35 U.S.C. §102(e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP §2131. Applicant traverses the rejection. Squilla fails to teach or suggest each and every claim element and fails to anticipate Claims 1-3, 5, 7-8, 12-13, and 21-23.

The rejected claims do not stand or fall together. The rejection of Claims 1-3, 5, 7-8, and 12-13 (Group I) are argued separately from Claims 21-23 (Group II).

2. Claims 1-3, 5, 7-8, and 12-13 (Group I)

Group I Claims Should Be Argued Separately

Claim 1 warrants separate argument. Claim 1 defines a method for authenticating a hardcopy document including recording a scanned representation of the hardcopy, generating lossy compressed image data, producing an

authentication token, and rendering at a printer a signed hardcopy document. Specific steps are not recited in the system claims of Group II. Moreover, the devices recited in the elements of the claims of Group II are untied to specific steps. Accordingly, Claim 1, and Claims 2-3, 5, 7-8, and 12-13, dependent thereon, should be reviewed separately.

Squilla Fails To Disclose Rendering At A Printer A Signed Hardcopy Document

Claim 1 recites arranging in a memory a scanned representation of a hardcopy document with a digital encoding of authentication data for rendering at a printer a signed hardcopy document. Squilla discloses authenticating digital images, particularly digital photographs, in *electronic* form. Squilla teaches an image format including a digital signature, image data, and location data for a selected image area that are stored in a digital file for later use, for example, in an insurance claim (Abstract, Col. 1, lines 34-41; Col. 3, lines 17-18; Fig. 5). During the digital signing process, a digital signature can be created directly from the digital image (Col. 5, lines 41-45) or from a scanned image of a hardcopy document (Col. 9, lines 26-28). During the authentication process, the image must be in its original digital form. The digital signature is attached to the digital file, which is stored on a removeable memory card or in a resident image memory (Col. 5, lines 34-40). Thus, the digital signature is stored electronically with the original digital file. Storing and transferring a digital signature and a digital image file differs from being able to arrange a hardcopy document with a digitally-encoded digital signature affixed to the document for rendering at a printer as a signed and authenticated hardcopy document, per Claim 1.

Additionally, rendering a printable hardcopy document, per Claim 1, offers an additional level of assurance that a digital file with a digital signature cannot. The hardcopy document provides for a regular handwritten signature and a digital signature, both which can be verified. Accordingly, rendering at a printer a signed hardcopy document, per Claim 1, is neither taught nor suggested by Squilla.

Squilla Fails To Disclose Hashed Encrypted Image Data Including Lossy Compressed Image Data And An Encrypted Hash Of The Lossy Compressed Image Data

Claim 1 recites an authentication token including hashed encrypted image data including lossy compressed image data and an encrypted hash of the lossy compressed image data. Squilla neither teaches nor discloses a digital signature that includes both the lossy compressed image data and an encrypted hash of the lossy compressed image data. In contrast, Squilla teaches compressing a selected region of a digital image, hashing the compressed region, and encrypting the hash to generate a digital signature (Col. 8, lines 34-51). The digital signature in Squilla contains a selected portion of the hashed compressed digital image (Col. 8, lines 35-40), rather than lossy compressed image data and an encrypted hash of the lossy compressed image data, per Claim 1.

A *Prima Facie* Case of Anticipation Has Not Been Met

Accordingly, a *prima facie* case of anticipation under 35 U.S.C. § 102(e) has not been shown with respect to independent Claim 1. Claims 2-3, 5, 7-8, and 12-13 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Moreover, Claim 2 recites recording a scanned representation of the signed hardcopy document. Claim 2 further recites comparing the signed hardcopy document with the authenticated lossy compressed image data to determine whether the signed hardcopy document is authentic. Squilla teaches storing the image and digital signature in a digital data file. The authentication process for verifying the digital signature is applied to the data file (Col. 8, lines 50-51) and not a scanned hardcopy document with an authentication token. Therefore, Squilla cannot teach recording a *signed hardcopy document* and comparing the *signed hardcopy document* with an authenticated lossy compressed image, per dependent Claim 2.

Moreover, Claim 3 recites visually comparing the signed hardcopy document with the authenticated lossy compressed image data. Squilla teaches appending the digital signature to a data image file for storing electronically.

Therefore, Squilla fails to teach visually comparing the *signed hardcopy document* with an authenticated lossy compressed image data.

Additionally, Claim 7 recites encoding the authentication token in embedded data, and Claim 8 recites encoding the authentication token in a halftone pattern. Squilla teaches compressing, hashing, and encrypting a selected portion of digital data (Col. 8, lines 44-47) without encoding the digital hashed data, per Claims 7 and 8. Squilla teaches using only a portion of the image for generating a digital signature to preserve the camera's power supply. Thus, Squilla fails to teach further encoding a digital signature in embedded data or in a halftone pattern, per Claims 7 and 8.

As a *prima facie* case of anticipation has not been established, withdrawal of the rejection of Claims 1-3, 5, 7-8, and 12-13 under 35 U.S.C. § 102(e) is respectfully requested.

3. Claims 21-23 (Group II)

Group II Claims Should Be Argued Separately

Claim 21 warrants separate argument. Claim 21 defines a system for authenticating a scanned representation of a hardcopy document that recites specific structural limitations such as an image compression module, an authentication token generator, and an encoding module. Analogous structural limitations are not recited in the method claims of Group I. Moreover, the steps recited in the claims of Group I are untied to specific structure. Accordingly, Claim 21, and Claims 22-23, dependent thereon, should be reviewed separately.

Squilla Fails To Disclose Rendering At A Printer A Signed Hardcopy Document

Claim 21 recites an encoding module for arranging a scanned representation of a hardcopy document with a digital encoding of authentication data for rendering at a printer a signed hardcopy document. Squilla discloses authenticating digital images, particularly digital photographs, in *electronic* form. Squilla teaches an image format including a digital signature, image data, and

location data for a selected image area that are stored in a digital file for later use, for example, in an insurance claim (Abstract, Col. 1, lines 34-41; Col. 3, lines 17-18; Fig. 5). During the digital signing process, a digital signature can be created directly from the digital image (Col. 5, lines 41-45) or from a scanned image of a hardcopy document (Col. 9, lines 26-28). During the authentication process, the image must be in a digital form. The digital signature is attached to the digital file, which is stored on a removeable memory card or in a resident image memory (Col. 5, lines 34-40). Thus, the digital signature is stored electronically with the digital file. Storing and transferring a digital signature and a digital image file differs from being able to arrange a hardcopy document with a digitally-encoded digital signature for rendering at a printer as a signed and authenticated hardcopy document, per Claim 21.

Additionally, rendering a printable hardcopy document, per Claim 21, offers an additional level of assurance that a digital file with a digital signature cannot. The hardcopy document provides for a regular handwritten signature and a digital signature, both which can be verified. Accordingly, rendering at a printer a signed hardcopy document, per Claim 21, is neither taught nor suggested by Squilla.

Squilla Fails To Disclose Hashed Encrypted Image Data Including Lossy Compressed Image Data And An Encrypted Hash Of The Lossy Compressed Image Data

Further, Claim 21 recites an authentication token including hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data. Squilla neither teaches nor discloses a digital signature that includes both the lossy compressed image data and an encrypted hash of the lossy compressed image data. In contrast, Squilla teaches compressing a selected region of a digital image, hashing the compressed region, and encrypting the hash to generate a digital signature (Col. 8, lines 34-51). The digital signature in Squilla contains only a selected portion of the hashed compressed digital image (Col. 8, lines 35-40), rather than lossy compressed

image data and an encrypted hash of the lossy compressed image data, per Claim 21.

A *Prima Facie* Case Of Anticipation Has Not Been Met

Accordingly, a *prima facie* case of anticipation under 35 U.S.C. § 102(e) has not been shown with respect to independent Claim 21. Claims 22 and 23 are dependent on Claim 21 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Moreover, Claim 22 recites recording the signed hardcopy document and comparing the signed hardcopy document with the authenticated hardcopy document to determine whether the signed hardcopy document is authentic. Squilla teaches storing the data image in a digital file including the complete unaltered image and the digital signature. Therefore, Squilla cannot teach recording a signed hardcopy document or comparing the signed hardcopy document with the authenticated lossy compressed image data, per Claim 22.

As a *prima facie* case of anticipation has not been established, withdrawal of the rejection of Claims 21-23 under 35 U.S.C. § 102(e) is respectfully requested.

G. Issue II

A *prima facie* case of obviousness under 35 U.S.C. § 103(a) has not been shown and the rejection of Claim 4 cannot stand.

1. Legal Basis

To establish a *prima facie* case of obviousness, the examiner has the burden of proving that (1) there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there is a reasonable expectation of success; and (3) the combined references teach or suggest all the claim limitations. MPEP § 2143. Failure to provide a suggestion or motivation to combine references cannot support a *prima facie* case of obviousness. MPEP § 2143.01. Applicant traverses the rejection. The

combination of the Squilla and Merkle references, fail to support a *prima facie* case of obviousness.

2. A *Prima Facie* Case Of Obviousness Has Not Been Shown

The first prong of *prima facie* obviousness requires some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings. Initially, the examiner must show some teaching or suggestion to combine references that supports their use in combination. *See*, *Ashland Oil, Inc. v. Delta Resins & Refracs., Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985). Such teaching or suggestion has not been shown.

Merkle teaches a system for authenticating a hardcopy document using a digital signature and a smart card, which identifies the person who supplies the hardcopy document to the printer (Merkle, Col. 4, lines 37-52). The output of the system is a digitally cleaned document that is an exact copy of the original document (Merkle, Col. 4, lines 18-23). In contrast, Squilla teaches selecting a region of interest of an image for use in a digital signature that is stored in a digital file with the unaltered image. A private key is embedded in a digital camera for use in subsequently verifying that a particular photo was taken on a particular camera (Squilla, Col. 7, lines 42-49). The identity of the person who took the picture is verified by his ownership of the camera and the digital authentication of the photo.

One of ordinary skill in the art would not find a suggestion or motivation to combine Squilla with Merkle. Squilla teaches a system for generating and attaching a digital signature to a digital image file, whereas Merkle teaches a system for printing a digitally cleaned hardcopy document. In particular, Squilla teaches an image format including a file header field with the location of a region of interest, a signature field with the digital signature, and a data field with the unaltered digital image (Squilla, Col. 5, lines 41-50). In contrast, the system in Merkle uses the literal scanned representation of a hard copy document. Templates are not created and stored in the system, and regions of interest are not

selected from the image for authentication. The Squilla and Merkle references are being improperly combined without a proper showing of a teaching or motivation to combine. MPEP § 2143.01. The system in Merkle generates a digitally cleaned hardcopy of the original document (Merkle, Col. 5, lines 36-45). Information needed to restore the original is digitally encoded on the copy and thus, a copier can determine what the original looked like (Merkle, Col. 5, lines 41-45). Thus, generating a digital signature based only on a region of interest as taught by Squilla, does not allow the system to generate a digitally cleaned document, as disclosed in Merkle. "The mere fact that prior art may be modified in the manner suggested by the examiner does not make the modification obvious unless the prior art suggests the desirability of the modification." *In re* Fritch, 974 F.2d 1260 (Fed. Cir. 1992).

Second, there would not be a reasonable expectation of success. The expectation of success must be founded in the prior art and not in the applicant's disclosure. *In re* O'Farrell, 853 F.2d 894 (Fed. Cir. 1988). Squilla teaches authenticating digital images using a region of interest, whereas Merkle teaches authenticating documents with a digital signature including the whole document. More specifically, Merkle teaches generating a digital signature including scanning and digitizing a document, and encrypting the digitized information with a secret key, whereas Squilla teaches generating a digital signature including only a region of interest that is compressed, hashed, and encoded for affixing to a digital file. Combining the teachings of Squilla with the teachings of Merkle would thus provide generating a digital signature with a selected region of interest of the document for authentication and printing a digitally cleaned version of the document using only a portion of the whole document. However, selecting only one portion of a text document may not include all of the significant information of the text document necessary for authentication. As a result, the combination of Squilla and Merkle would not suggest to one of ordinary skill in the art that the combined process should be carried out or that the combined process would have a likelihood of success.

Finally, the combined Squilla and Merkle references fail to teach or

suggest all the claim limitations. Claim 4 recites visually comparing the signed hardcopy document with a printed hardcopy document of the authenticated lossy compressed image data. Merkle teaches a system for authenticating documents using a checking algorithm that determines whether the digital signature on the signed hardcopy document corresponds to the information obtained directly from the original document and the outcome of the checking algorithm is a single bit indicating that the signature is valid or invalid (Merkle, Col. 3, line 64-Col. 5, line10). If the signature is valid, the system prints a digitally cleaned document and, if the signature is invalid, the system is programmed not to copy the document (Merkle, Col. 6, line 61-Col. 7, line 4). The recipient of a signed hardcopy could easily verify that the signature is authentic by placing the document into a signing copier (Merkle, Col. 8, lines 34-36), rather than visually verifying the signed hardcopy document with a printed hardcopy document, per Claim 4.

Further, as described above with reference to the rejection under 35 U.S.C. § 102(e) of Claims 1-3, 5, 7-8, 12-13, and 21-23, the base reference, Squilla, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claim 4 is dependent on Claim 1 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Withdrawal of the rejection under 35 U.S.C. § 103(a) is respectfully requested.

H. Issue III

A *prima facie* case of obviousness under 35 U.S.C. § 103(a) has not been shown and the rejection of Claims 6 and 9-11 cannot stand.

As described above with reference to the rejection under 35 U.S.C. § 102(e) of Claims 1-3, 5, 7-8, 12-13, and 21-23, the base reference, Squilla, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claims 6 and 9-11 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further

distinguished by the limitations recited therein. Accordingly, the Squilla and Curry references, taken as a whole, fail to teach or suggest the claimed subject matter of Claims 6 and 9-11. As the combination of the Squilla and Curry references fail to render Claims 6 and 9-11 obvious, withdrawal of the rejection under 35 U.S.C. § 103(a) is requested. Withdrawal of the rejection under 35 U.S.C. § 103(a) is respectfully requested.

I. Issue IV

A *prima facie* case of obviousness under 35 U.S.C. § 103(a) has not been shown and the rejection of Claims 14-17 cannot stand.

The first prong of *prima facie* obviousness requires some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings. Initially, the examiner must show some teaching or suggestion to combine references that supports their use in combination. *See, Ashland Oil, Inc. v. Delta Resins & Refracs., Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985). Such teaching or suggestion has not been shown.

Zdybel teaches combining hardcopy output and electronic documents into a lossless communications medium (Zdybel, Abstract; Col. 4, lines 20-41) by encoding bit-level digital data content into glyph encodings (Zdybel, Col. 8, lines 38-50). The glyph encodings are not encoded or intended to provide authentication of the underlying hardcopy document. Rather, the glyph encodings represent the digital data content of ASCII, DDL or PDL encodings, which are determined by using recognition software to extract semantic information in the form of bit-level digital data contents from a document (Zdybel, Col. 7, line 66-Col. 8, line 4). A machine readable digital representation and a human readable rendering are then created on the same recording media using the same printing process (Zdybel, Col. 4, lines 45-51).

Squilla teaches authenticating a document by selecting a region of interest from a digital image for generating a digital signature. The selected region is compressed, hashed, encrypted with a private key, and appended to a digital file (Col. 6, line 65-Col. 7, line 58). The digital signature is not generated to produce

a digital representation of the original photograph. Rather, the digital signature provides authentication of the photograph for determining the source of the photograph.

One of ordinary skill in the art would not find a suggestion or motivation to modify or combine Squilla with Zdybel. Squilla teaches a process of validation that generates a digital signature for authenticating digital images. Zdybel teaches robust and reliable recovery of information carried in hardcopy documents for transformation to an electronic format. Thus, the Squilla and Zdybel references are being improperly combined without a proper showing of a teaching or motivation to combine. MPEP § 2143.01. "The mere fact that prior art may be modified in the manner suggested by the examiner does not make the modification obvious unless the prior art suggests the desirability of the modification." *In re* Fritch, 974 F.2d 1260 (Fed. Cir. 1992).

Second, there would not be a reasonable expectation of success. The expectation of success must be founded in the prior art and not in the applicant's disclosure. *In re* O'Farrell, 853 F.2d 894 (Fed. Cir. 1988). Zdybel teaches encoding bit-level digital data content into glyph encodings that can be used to recover data, whereas Squilla teaches authenticating a photograph by generating a digital signature including a region of interest that is compressed, hashed, and encoded for affixing to a digital file. Combining the teachings of Squilla with the teachings of Zdybel would thus provide a document that substitutes a digital signature with glyph encodings for authenticating documents. However, the glyph encodings of Zdybel are unable to verify the source of a document because information regarding sender source is not entered into the system for encoding and the combination of Squilla and Zdybel would not suggest to one of ordinary skill in the art that the combined process should be carried out or that the combined process would have a reasonable likelihood of success.

Finally, the combined Squilla and Zdybel references fail to teach or suggest all the claim limitations. Claim 14 recites recording exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document. Claim 15 recites recording the locations of exemplars at

a resolution that is less than the selected resolution of the scanned representation of the hardcopy document. Zdybel fails to teach recording exemplars or exemplar locations at a resolution that is less than a selected resolution of a scanned representation of a hardcopy document. In contrast, Zdybel teaches converting scanned text into a bitmap of textual encodings and further encoding the bitmap into glyph encodings including information specific to the document. All or a selected portion of the digital encodings from an electronic document is printed on a hardcopy document (Zdybel, Col. 9, lines, 38-41). Recording and storing the scanned information of Zdybel at a resolution less than the selected resolution of the scanned representation of the document makes recognition and recovery difficult. Thus, Zdybel fails to teach recording exemplars or exemplar locations at a resolution that is less than a selected resolution of a scanned representation of a hardcopy document.

Moreover, Claim 16 recites compressing identified portions of the image data at a plurality of compression ratios. Zdybel neither teaches nor discloses compressing data at a plurality of compression ratios. Rather, Zdybel teaches scanning a hardcopy document to produce an electronic bitmap representation of the document, further converting the bitmap representation into elemental textual and graphical encodings, and finally converting the bit-level encodings into glyph encodings (Zdybel, Col. 7, line 62-Col. 8, line 47). The system in Zdybel fails to include the additional step of compressing the electronic bitmap at different ratios, per Claim 16.

Further, as described above with reference to the rejection under 35 U.S.C. § 102(e) of Claims 1-3, 5, 7-8, 12-13, and 21-23, the base reference, Squilla, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claims 14-17 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Squilla and Zdybel references, taken as a whole, fail to teach or suggest the claimed subject matter of Claims 14-17. As Squilla and Zdybel fail to render Claims 14-17

obvious, withdrawal of the rejection under 35 U.S.C. § 103(a) is requested.

J. Issue V

A *prima facie* case of obviousness under 35 U.S.C. § 103(a) has not been shown and the rejection of Claims 18-20 cannot stand.

The first prong of *prima facie* obviousness requires some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings. Initially, the examiner must show some teaching or suggestion to combine references that supports their use in combination. *See*, *Ashland Oil, Inc. v. Delta Resins & Refracs., Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985). Such teaching or suggestion has not been shown.

Walker teaches entering selected variable information from a hardcopy document into an authentication system. The selected document data is processed using a private key to generate a unique encrypted code, which is affixed to the hardcopy document (Walker, Col. 5, lines 9-11). In contrast, Squilla teaches capturing an image, selecting a region of interest, compressing and hashing the region of interest, and encrypting the hash for appending to a digital image file.

One of ordinary skill in the art would not find a suggestion or motivation to modify or combine Squilla with Walker. Squilla teaches a process of validation that requires a digital image, whereas Walker teaches a process of entering selected variable information from a hardcopy document into the system. The selected variable data in Walker is inputted in the authentication system using a keypad (Walker, Col. 5, lines 1-4), rather than converting the complete hardcopy document to a digital document and then selecting the variable data for use in the digital signature, as in Squilla. The digital signature is appended to a data image file, whereas Walker teaches stamping the digital signature on a hardcopy document or printing the digital signature on a label. Thus, the Squilla and Walker references are being improperly combined without a proper showing of a teaching or motivation to combine. MPEP § 2143.01. "The mere fact that prior art may be modified in the manner suggested by the examiner does not make the modification obvious unless the prior art suggests the desirability of the

modification." *In re* Fritch, 974 F.2d 1260 (Fed. Cir. 1992).

Second, there would not be a reasonable expectation of success. The expectation of success must be founded in the prior art and not in the applicant's disclosure. *In re* O'Farrell, 853 F.2d 894 (Fed. Cir. 1988). Squilla teaches authenticating digital images, whereas Walker teaches authenticating and verifying text documents. More specifically, Walker teaches generating a digital signature and stamping or printing a label with the digital signature for placement on a hardcopy document, whereas Squilla teaches generating a digital signature including a region of interest that is compressed, hashed and encoded for affixing to a digital file. Combining the teachings of Squilla with the teachings of Walker would thus provide, entering selected information from a printed photograph into the authentication system and processing the selected photo data using a private key to generate a unique encrypted code. However, entering and recognizing selected data from a text hardcopy document differs from entering and recognizing selected data from a printed hardcopy photograph, and, as a result, the combination would fail to provide a method for authenticating a hardcopy document, per Claims 18-20.

Finally, the combined Squilla and Walker references fail to teach or suggest all the claim limitations. Claim 18 recites recording a scanned representation of the hardcopy document at a selected resolution, generating lossy compressed image data, producing an authentication token, and arranging a digital encoding of the authentication data for rendering at a printer a label containing the digital encoding of the authentication data. The authentication token includes one of encrypted image data and hashed encrypted image data; the hashed encrypted image data includes the lossy compressed image data and an encrypted hash of the lossy compressed image data. Squilla neither teaches nor discloses an authentication token that includes both the lossy compressed image data and an encrypted hash of the lossy compressed image data. In contrast, Squilla teaches compressing a selected region of a digital image, hashing the compressed region, and encrypting the hash to generate a digital signature (Col. 8, lines 34-51). The digital signature in Squilla contains only a selected portion of the hashed

compressed digital image (Col. 8, lines 35-40), rather than the whole document as lossy compressed image data and an encrypted hash of the lossy compressed image data, per Claim 18. Selecting a portion of the digital image reduces the power requirements for subsequent hashing and encryption (Col. 4, lines 30-34). Thus, a digital signature including compressed image data and an encrypted hash of compressed image data requires additional power and memory. Therefore, Squilla fails to teach a digital signature that includes both the lossy compressed image data and an encrypted hash of the lossy compressed image data.

Claims 19 and 20 are dependent upon Claim 18 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of rejection under 35 U.S.C. § 103(a) is respectfully requested.

In closing, Applicant respectfully submits that the rejections under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a) cannot be sustained in view of the foregoing arguments and should be withdrawn. As this Appeal Brief seeks to reinstate the earlier appeal of December 5, 2003, the required Appeal Brief fee has been already paid. No Appeal Brief fee is due. Appellant's undersigned attorney can be reached at (206) 381-3900.

Dated: November 14, 2006

By: _____
Patrick J.S. Inouye, Esq.
Reg. No. 40,297

Cascadia Intellectual Property
500 Union Street
Suite 1005
Seattle, WA 98101

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

8. CLAIMS APPENDIX

1. (Previously amended) A method for authenticating a hardcopy document, comprising the steps of:

recording in a memory a scanned representation of the hardcopy document at a selected resolution;

generating lossy compressed image data with the scanned representation of the hardcopy document;

producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

arranging in the memory the scanned representation of the hardcopy document with a digital encoding of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

2. (Original) The method according to claim 1, further comprising the step of verifying the signed hardcopy document by:

recording a scanned representation of the signed hardcopy document;

decoding the authentication token from the scanned representation of the signed hardcopy document;

authenticating the lossy compressed image data using one of the encrypted image data and the hashed encrypted image data; and

decompressing the authenticated lossy compressed image data for comparison with the signed hardcopy document to determine whether the signed hardcopy document is authentic.

3. (Original) The method according to claim 2, further comprising the step of visually comparing the signed hardcopy document with the authenticated lossy compressed image data.

4. (Original) The method according to claim 2, further comprising the step of visually comparing the signed hardcopy document with a printed hardcopy document of the authenticated lossy compressed image data.

5. (Original) The method according to claim 2, wherein said step of producing an authentication token is performed with a private key and said step of authenticating lossy compressed image data is performed with a public key.

6. (Original) The method according to claim 1, further comprising the step of encoding the authentication token in a low intensity background pattern.

7. (Original) The method according to claim 1, further comprising the step of encoding the authentication token in embedded data.

8. (Original) The method according to claim 7, wherein said encoding step encodes the authentication token in a halftone pattern.

9. (Original) The method according to claim 8, wherein said encoding step encodes the authentication token in a hyperbolic halftone pattern.

10. (Original) The method according to claim 8, wherein said encoding step encodes the authentication token in a serpentine halftone pattern.

11. (Original) The method according to claim 7, wherein said encoding step encodes the authentication token in data glyphs.

12. (Original) The method according to claim 1, wherein said step of generating lossy compressed image data loses document formatting contained in the scanned representation of the hardcopy document.

13. (Original) The method according to claim 12, wherein said step of generating lossy compressed image data further comprises the step of compressing the scanned representation of the hardcopy document by identifying exemplars and locations of exemplars; each exemplar identified representing one

or more image segments from the scanned representation of the hardcopy document.

14. (Original) The method according to claim 13, wherein said compressing step records the exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document.

15. (Original) The method according to claim 13, wherein said compressing step records that locations of exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document.

16. (Original) The method according to claim 1, wherein said compressing step compresses identified portions of the image data at a plurality of compression ratios.

17. (Original) The method according to claim 16, further comprising the step of segmenting text data from pictorial data before compressing the scanned representation of the hardcopy document.

18. (Original) A method for authenticating a hardcopy document, comprising the steps of:

recording in a memory a scanned representation of the hardcopy document at a selected resolution;

generating lossy compressed image data with the scanned representation of the hardcopy document;

producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

arranging in the memory a digital encoding of the authentication data for rendering at a printer a label containing the digital encoding of the authentication data.

19. (Original) The method according to claim 18, further comprising the step of fixedly attaching the label to the hardcopy document to produce a signed hardcopy document.

20. (Original) The method according to claim 19, further comprising the step of verifying the signed hardcopy document by:

recording a scanned representation of the signed hardcopy document;

decoding the authentication token from the scanned representation of the signed hardcopy document;

authenticating the lossy compressed image data using one of the encrypted image data and the hashed encrypted image data; and

decompressing the authenticated lossy compressed image data for comparison with the signed hardcopy document to determine whether the signed hardcopy document is authentic.

21. (Previously amended) A system for authenticating a scanned representation of a hardcopy document, comprising:

an image compression module for generating lossy compressed image data with the scanned representation of the hardcopy document;

an authentication token generator for producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

an encoding module for arranging the scanned representation of the hardcopy document with a digital encoding of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

22. (Previously amended) The system according to Claim 21, further comprising:

a memory for recording the signed hardcopy document;

a decoding module for decoding the signed hardcopy document to define decoded signed image data;

an authentication module to authenticating the decided signed image data using of the encrypted image data and the hashed encrypted image data to define authenticated image data; and

a decompression module for decompressing the authenticated image data to define decompressed image data;

means for comparing the signed hardcopy document with the authenticated hardcopy document to determine whether the signed hardcopy document is authentic.

23. (Previously amended) The system according to Claim 21, wherein said image compression module compresses the scanned representation of the hardcopy document by identifying exemplars and locations of exemplars; each exemplar identified representing one or more image segments from the scanned representation of the hardcopy document.

9. EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None.